TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/04/2020

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Android OS builds utilizing Security Patch Levels issued prior to August 5, 2020.

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**
Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**
Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for remote code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could allow for Escalation of Privileges (CVE-2020-0238, CVE-2020-0257)
- A vulnerability in Framework that could allow for Remote Code Execution (CVE-2020-0240)
- Multiple vulnerabilities in Framework that could allow for Information Disclosure (CVE-2020-0239, CVE-2020-0249, CVE-2020-0258)
- A vulnerability in Framework that could allow for Denial of Service (CVE-2020-0247)
- Multiple vulnerabilities in Media Framework that could allow for Escalation of Privileges (CVE-2020-0241, CVE-2020-0242, CVE-2020-0243)
- Multiple vulnerabilities in System that could allow for Escalation of Privileges (CVE-2020-0108, CVE-2020-0256)
- Multiple vulnerabilities in System that could allow for Information Disclosure (CVE-2020-0248, CVE-2020-0250)
- A vulnerability in Google Play system updates that could allow for Escalation of Privileges (CVE-2020-0259)
- A vulnerability in AMLogic components that could allow for Escalation of Privileges (CVE-2020-0259)
- Multiple vulnerabilities in Kernel components that could allow for Escalation of Privileges (CVE-2020-0255, CVE-2020-12464)
- A vulnerability in Kernel components that could allow for Information Disclosure (CVE-2019-16746)
- Multiple vulnerabilities in MediaTek components that could allow for Escalation of Privileges (CVE-2020-0252, CVE-2020-0253, CVE-2020-0260)
- Multiple vulnerabilities in MediaTek components that could allow for Information Disclosure (CVE-2020-0251, CVE-2020-0254)
- Multiple High severity vulnerabilities in Qualcomm components (CVE-2020-11115, CVE-2020-11118, CVE-2020-11120)
- A Critical severity vulnerability in Qualcomm components (CVE-2020-11116)
- Multiple High severity vulnerabilities in Qualcomm closed-source components (CVE-2018-5886, CVE-2018-13903, CVE-2019-13999, CVE-2019-14025, CVE-2019-14052, CVE-2019-14056, CVE-2019-14065, CVE-2019-14089, CVE-2019-14115, CVE-2019-14119, CVE-2020-3611, CVE-2020-3624, CVE-2020-3636, CVE-2020-3640, CVE-2020-3643, CVE-2020-3644, CVE-2020-3666, CVE-2020-3668, CVE-2020-3669, CVE-2020-3675, CVE-2020-11122, CVE-2020-11128)
- Multiple Critical severity vulnerabilities in Qualcomm closed-source components (CVE-2019-10562, CVE-2019-10615, CVE-2019-13998, CVE-2020-3619, CVE-2020-3667)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of a privileged process. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions be taken:
- Apply appropriate updates by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.

- Remind users to only download applications from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

REFERENCES:

Google Android:
https://source.android.com/security/bulletin/2020-08-01

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13903
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5886
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10562
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10615
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13998
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13999
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14025
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14052
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14056
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14065
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14089
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14115
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16746
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0108
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0238
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0239
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0240
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0241
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0242
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0243
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0247
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0248
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0249
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0250
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0251
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0252
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0253
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0255
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0256
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0257
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0258
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0259
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0259
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0260
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11115
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11116
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11118

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11120
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11122
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11128
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12464
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3611
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3619
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3624
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3636
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3640
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3643
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3644
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3666
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3667
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3668
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3669
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3675